2021/4/5
الخميس

الموضوع: محاضرة (2) نظري

$a \equiv b (\bmod m)$
$m \mid (a-b)$
$15 \equiv 8 (\bmod 7)$
$(3)^2 \equiv 1 (\bmod 4)$

تمرين: لدينا عدد صحيح $a \in \mathbb{Z}$

(1) اثبت أن باقي قسمة مربع أي عدد صحيح على (4) إما (0) أو (1)

$$a^2 \equiv 0 \text{ or } 1 \pmod 4$$

(2) إذا كان n عدد طبيعي أكبر من (1) تحتوي كل العدد في جميع مراتبه العشرية فبرهن أنه لا يكون مربعاً كاملاً.

(أي لا يمكن إيجاد عدد صحيح مربعه هو ذلك العدد (111111....))

الحل: عند تقسيم a على 4 نحصل على احدى الحالات التالية:

$$a = 4q \Rightarrow a^2 = 16q^2 = 4(\underbrace{4q^2}_{k})$$

$$a = 4q+1 \Rightarrow a^2 = 16q^2 + 8q + 1 = 4(\underbrace{4q^2 + 2q}_{k \in \mathbb{Z}}) + 1$$
$$= 4k+1$$

$$a = 4q+2 \Rightarrow a^2 = 16q^2 + 16q + 4 = 4(\underbrace{4q^2 + 4q + 1}_{k})$$
$$= 4k+1$$

$$a = 4q+3 \Rightarrow a^2 = 16q^2 + 24q + \underset{8+1}{9} = 16q^2 + 24q + 8 + 1$$
$$= 4(\underbrace{4q^2 + 8q + 2}_{k}) + 1 = 4$$

2. n عدد طبيعي أكبر من الواحد (n>1) جميع مراتبه واحدات

$$n = 111 \text{------} 1111$$
$$= 111 \text{------} 100 + 11$$

(نحصل القسمة على 4 الباقي 0)

$$= 4q + 8 + 3$$
$$= 4(q+2) + 3 = 4k + 3 \quad \text{و} \quad k = q+2 \in \mathbb{Z}$$

$$\boxed{n = 4k + 3}$$

باقي قسمة n على (4) هو (3) أي لا يساوي (0) أو (1)

ومن ثم n ليس مربعاً كاملاً، وأنه لا يمكن ايجاد عدد صحيح مربعه يساوي n

الفصل الأول انتهى

الفصل الثاني

القواسم المشتركة والمضاعفات المشتركة

تعريف: نقول ان العدد الصحيح $d_1 \neq 0$, $d_1 \in \mathbb{Z}$ إنه قاسم مشترك للعددين الصحيحين a و $b \in \mathbb{Z}$ غير الصفريين إذا كان $d_1 | a$ ∧ $d_1 | b$.

ملاحظات:

- إذا كان $(d_1 | a)$ و $(d_1 | b)$ فإن $(-d_1 | a)$ ∧ $(-d_1 | b)$
- إن القاسم المشترك d_1 بالقيمة المطلقة لا يتجاوز العدد الأصغر بين العددين $|a|$ و $|b|$. $a.b \neq 0$ ؛ $|d_1| \leq |a|$ ، $|d_1| \leq |b|$
- إن مجموعة القواسم المشتركة الموجبة لعددين صحيحين غير صفريين هي تقاطع مجموعة القواسم الموجبة لـ a مع مجموعة القواسم الموجبة لـ b فهي حتماً مجموعة منتهية .

تعريف: القاسم المشترك الأعظم:

نقول أن العدد d هو القاسم المشترك الأعظم للعددين a و b غير الصفريين

$$gcd(a,b) = d = d(a,b) = (a,b)$$

إذا كان

1) $d > 0$
2) $d | a$ ∧ $d | b$
3) إذا وجد قاسم آخر a و b مثل $c > 0$ بحيث $c | a$ و $c | b$ فإن $c \leq d$

ينتج مباشرة من هنا ومن الملاحظة (*) أن القاسم المشترك الأعظم لعددين غير صفريين موجود دائماً ووحيد

ملاحظة: إذا كان $a = b = 0$ فإن مجموعة القواسم المشتركة هي كل $\mathbb{Z}$ فهي مجموعة غير منتهية وليس فيها عنصر أكبر ومن ثم لا يوجد قاسم مشترك أعظم

/ /

الموضوع:

القاسم المشترك

مبرهنة: إذا كان a, b عددين صحيحين غير معدومين فإن القاسم المشترك الأعظم لهما هو تركيب خطي لهذا العددين.

أي يوجد دائماً عددان صحيحان:

$\exists x_0, y_0 \in \mathbb{Z} : d(a,b) = d = ax_0 + by_0$

مثال: $d(12,15) = 3$

$3 = (-1)12 + (1)15$

أو $(-6)12 + (5)15$

ملاحظة: إن القاسم المشترك الأعظم لعددين غير معدومين هو العنصر الأصغر لمجموعة التراكيب الخطية الموجبة للعددين a و b.

نتيجة: إذا كان c قاسم لـ a و b فهو حتماً قاسم لـ $d(a,b)$

تعريف: إذا كان القاسم المشترك الأعظم لعددين صحيحين يساوي (1) فإننا نسمي هذين العددين أوليان نسبياً فيما بينهما

مبرهنة في هذه الحالة الآتي:

يكون العددان a و b غير المعدومين أوليين نسبياً فيما بينهما إذا وفقط إذا وجد عددان صحيحان x و y بحيث أن $ax + by = 1$

إثبات:

($\Leftarrow$) نفرض أن a, b أوليان فيما بينهما $d = (d(a,b) = 1)$

وحسب مبرهنة سابقة، يوجد عددان صحيحان x_0 و y_0 بحيث أن

$ax_0 + by_0 = 1$

($\Rightarrow$) نفرض الآن وجود عددان صحيحان x و y بحيث أن

$x, y \in \mathbb{Z}$ ؛ $ax + by = 1$

وليكن $d = d(a,b)$ أي أن $d | a \wedge d | b \Leftarrow$

$d | (ax + by) = 1 \Rightarrow d = 1$

أي أن العددين a و b أوليان نسبياً فيما بينهما.

ينتج من هذا مباشرة.

نتيجة: إذا كان $d = d(a,b)$

$$\Rightarrow d\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

تمرين: اثبت أن القاسم المشترك لـ b, a

$$d(a,b) = d(a, b-ac)$$

بعض خواص القاسم المشترك.

1) $d(-a,-b) = d(a,b) \Rightarrow d(a,-b) = d(-a,b)$

$= d(|a|,|b|) = d(a,b)$

2) $d(1,a) = 1$

$d(0,a) = |a|$

3) $d(a,m) = d(b,m) = 1$

$\Rightarrow d(a.b, m) = 1$

القاسم المشترك الأعظم لجدائهما (1) طالما أنهما أولي مع m

4) $d(k,b) = 1 \;\wedge\; k \mid (a.b)$

$\Rightarrow k \mid a$

k يقسم جداء العددين a,b
وإذا كان بينهما أولياً مع أحد العددين
فإنه يقسم العدد الآخر

إذا كان p عدد أولياً ويقسم جداء العددين a و b فإنه يقسم أحدهما

$p \mid a.b \Rightarrow p \mid a$ or $p \mid b$

ملاحظة: $4 \mid 12 = 2.6$; $4 \nmid 2$, $4 \nmid 6$ || $4 \mid 12 = 3.4$; $d(4,3) = 1 \Rightarrow 4 \mid 4$

شرط أساسي يجب أن يكون k أولياً مع أحد العددين.

5) $d = d(a,b) \Rightarrow d(ma, mb) = m.d$

اثبت ذلك

صـ 90 كتاب

الموضوع:

خوارزمية إقليدس:

مبرهنة: إذا كان $0 < r < a$ عدد صحيح

وكان $b = qa + r$ و $0 < r < a$ فإن

$d(b, a) = d(a, r)$

$d(a, b) = d \Rightarrow d | a \wedge d | b$

$\Rightarrow d | (b + (-qa)) = r$

نستنتج: كل قاسم مشترك لـ (a, b) هو قاسم مشترك لـ (a, r)

كل قاسم مشترك لـ a, b يجب أن يقسم r، أي أن d يقسم r

لنأخذ c عدد ما، بحيث أن c قاسم لـ a, r فهو قاسم لـ $qa + r$

أي c قاسم لـ b

وحيث أن c قاسم لـ a بالفرض $\Leftarrow$ $c | d$

أي أن القاسم المشترك الأعظم لـ a, r هو نفسه d

خوارزمية إقليدس:

هي وسيلة لإيجاد القاسم المشترك الأعظم لعددين صحيحين وكتابته أيضاً كتركيب خطي لهما، ويتم ذلك وفق عمليات قسمة متتالية.

وحيث أن $d(a, b) = d(|a|, |b|)$ فيمكن أن نفترض دوماً أن العددين موجبات تماماً.

أي للبحث عن القاسم المشترك الأعظم لعددين موجبين نطبق خوارزمية القسمة بشكل متتالٍ حتى نصل إلى الباقي الصفري ويكون عندئذٍ الباقي الأخير قبل الباقي الصفري هو القاسم المشترك الأعظم الذي نبحث عنه.

والمثال التالي يوضح ذلك:

اكتب القاسم المشترك الأعظم للعددين $\overset{b}{72}$ ، $\overset{a}{30}$ كتركيب خطي لهما

$72 = 2 \boxed{30} + 12$

نقسم a على الباقي $30 = 2 \cdot \boxed{12} + 6$ ، القاسم المشترك الأعظم لهما

$12 = 2 \boxed{6} + 0$

$6 = 30 - 2 \cdot \boxed{12} = 30 - 2(72 - 2 \cdot \boxed{30})$

$6 = \underline{5}(30) + (\underline{-2})\, 72$

x_0 y_0

1 / 1 الموضوع :

مثال: اكتب القاسم المشترك الأعظم للعددين 20 ، 172 كتركيب خطي لهما

$$\left.\begin{aligned} 172 &= 8 \cdot 20 + 12 \\ 20 &= 1 \cdot 12 + 8 \\ 12 &= 1 \cdot 8 + \boxed{4} \\ 8 &= 2 \cdot 4 + 0 \end{aligned}\right\} \Rightarrow d(172, 20) = 4$$

$$4 = 12 - 1 * 8 = 12 - 1 * [20 - 1 * 12]$$
$$= 2(12) - 20$$
$$= 2[172 - 8 * 20] - 1 * 20$$
$$\boxed{4 = 2(172) + (1-17)(20)}$$

تمرين: اكتب القاسم المشترك الأعظم للعددين 3054 و 1237 كتركيب خطي لهما.

تمرين: أوجد القاسم المشترك الأعظم $d > 0$ بحيث يكون $d \mid 18$ ∧ $d \nmid 12$ و $\frac{36}{d} \nmid 10$

[نجزئ قواسم الـ 12 ونجزئ قواسم الـ 18 ونقسمها ثم نخرج القواسم $\frac{36}{d}$] طريقة الحل

يعرف القاسم المشترك الأعظمي لمجموعة أعداد صحيحة ليست جميعها أصفار بتعميم التعريف السابق

أي ، $a_i \in \mathbb{Z}$; $i = 1 - n$

1) $d > 0$

2) $d \mid a_i$; $\forall i = 1, 2 - n$

3) $c > 0$; $c \mid a_i \Rightarrow c \leq d$

ويقال أن الأعداد $a_i (i = 1 - n)$ أولية نسبياً إذا كان القاسم المشترك الأعظمي

لهذه الأعداد يساوي (1).

ويقال أنها نسبية أولياً مثنى مثنى ، إذا كان القاسم المشترك الأعظمي لأي

اثنين منها هو (1).

$d(6, 8, 15) = 1$ أولية نسبياً

$d(6, 8) = 2$ ليست أولية نسبياً مثنى مثنى

ملاحظة ع الهامش: إذا كانت نسبية مثنى مثنى فهي نسبية أما العكس غير صحيح.
إذا كانت نسبية ليس بالضرورة أنها نسبية مثنى مثنى

المضاعف المشترك الأصغر

$lcm(a,b) = L(a,b) = [a,b]$

تعريف: لتكن a_i أعداد صحيحة غير صفرية $(i=1 \dots n)$

نقول أن العدد m مضاعف مشترك لهذه الأعداد إذا كان مضاعفاً لكل منها.

أي أن $a_i | m \quad (\forall i=1 \dots n)$

ونقول أن العدد L هو المضاعف المشترك الأصغر لهذه الأعداد $a_i \quad (i=1 \dots n)$

إذا كان:

1) $L > 0$

2) $a_i | L \quad \forall i=1 \dots n$

3) إذا كان $0 < m$ بحيث $a_i | m$ لكل $(i=1 \dots n)$

فإن $L \leq m$

ينتج مما سبق من هذا: أن المضاعف المشترك الأصغر هو أصغر المضاعفات المشتركة

وأن المضاعف المشترك الأصغر يقسم أي مضاعف آخر لهذه الأعداد

جديد من الدكتور

إذا كان a,b عددين صحيحين موجبين وكان

$$\left.\begin{array}{l} d(a,b) = d \\ L(a,b) = L \end{array}\right\} \Rightarrow d \cdot L = a \cdot b$$

أي: $L(a,b) = \dfrac{a \cdot b}{d(a,b)}$

أي:

$$gcd(a,b) \cdot lcm(a,b) = (a \cdot b)$$

إثبات المبرهنة صفحة 45 كتاب

نتيجة: إذا كان a,b أوليان فيما بينهما $d(a,b)=1$

فإن $lcm = a \cdot b$

الفصل الثاني انتهى

/ /

الموضوع: الفصل الثالث

الأعداد الأولية وبعض خواصها.

. نقول ان العدد p أولي إذا كان $p>1$ وكان لا يقبل القسمة إلا على نفسه أو على الـ(1)
. p ملك ما سمي قسمته فقط هي (p ,1) ، وفيما عدا ذلك يدعى عدداً مؤلفاً (مركب)
. ويسمى العدد الصحيح الموجب غير الأولي والأكبر من (1) بأنه عدد مؤلف.

$n = a \cdot b$ ؛ $1<a<n$
$1<b<n$

بعض الخواص الأساسية:

1/ إن الأعداد الأولية هي أعداد أولية نسبياً مثنى مثنى. (2,3,5,7)

2/ إذا كان p يقسم n $(p|n)$ فإن $d(p,n) = p$
. وإذا لم يقسم $(p\nmid n)$ فإن $d(p,n)=1$

3/ إذا كان p عدد أولي وقسم جداء عددين صحيحين فهو حتماً يقسم أحد العددين
. $p|a \cdot b \Leftarrow p|a$ or $p|b$
$p|a_1 \cdot a_2 \cdots a_n \Leftarrow$ فإن p يقسم أحد المضاريب على الأقل

. نتيجة: إذا كانت $p|a_1 a_2 \cdots a_n$ وكانت a_i أعداد أولية
. فإن العدد الأولي p يساوي أحد المضاريب على الأقل (إذا كانت أولية)

المبرهنة الأساسية في الحساب:

. أي عدد صحيح $1<n \in \mathbb{Z}$ هو إما عدد أولي أو أنه جداء عدد منتهي من الأعداد
. الأولية ، وهذا التمثيل كجداء عوامل أولية يكون وحيداً بغض النظر (بإهمال ترتيب المضاريب)

$12 = 2^2 \cdot 3$

ملاحظة: يمكن أن تكون بعض العوامل الأولية لعدد صحيح متساوية ، فإذا جمعنا معاً العوامل
المتساوية أمكننا كتابة العدد n كجداء عوامل أولية بالشكل القانوني الآتي:

العبارة القانونية لـ n: $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ ؛ $p_1<p_2< \cdots <p_k$ و $\alpha_i \geq 0$
جميعها أعداد أولية.

$12 = 2 \cdot 3 = 2 \cdot 2 \cdot 3$

نتيجة: كل عدد صحيح $1<n$ له عامل أولي

الموضوع:

نتيجة: إذا كان $n>1$ عدد مؤلفاً (ليس أولي) فيوجد له عامل أولي حتماً أصغر من جذره (حتماً يوجد له عامل أولي مثل p بحيث أن $p \leq \sqrt{n}$ فيوجد $p|n$)

الإثبات: بما أن n مؤلف (جداء عددين)

$$n = a.b \; ; \; 1 < a \leq b < n$$

عندئذ

$$n = a.b \geq a^2$$

$$\sqrt{n} \geq a$$

لأن $a>1$ حسب نتيجة سابقة يوجد لها على الأقل عامل أولي مثل p بحيث أن

$$p|a \Leftarrow p|n = a.b$$

لأن p يقسم a فهو أصغر أو يساوي a $\quad p \leq a$

ولأن $a \leq \sqrt{n} \Leftarrow p \leq \sqrt{n}$

نتيجة: إذا كان $n>1$ وليس له عامل أولي أصغر أو يساوي جذره (n) $(p \leq \sqrt{n})$

حتماً يكون n عدداً أولياً.

طريقة الجذر [illegible]

تمرين: بين إن كان العدد (731) عدداً مؤلفاً أم عدداً أولياً [illegible]

دورة **تمرين:** اثبت أن p عدد أولي يقسم $p|\binom{p}{j} \; ; \; 1<j<p$

الحل: نناقش $\binom{p}{j}$

$$\binom{p}{j} = \frac{p!}{j!\,(p-j)!} = \frac{p(p-1) \cdots (p-j+1)(p-j)!}{j! \; (p-j)!}$$

$$= \frac{p(p-1) \cdots (p-j+1)}{j!}$$

ننقل $j!$ إلى الطرف الثاني

$$j!\binom{p}{j} = p(p-1) \cdots (p-j+1)$$

p يقسم الطرف الأيسر بالتالي

$$p \mid j!\binom{p}{j}$$

p أولي ويقسم جداء عددين فهو يقسم أحد المقدارين

لو كان $p \mid j! = j(j-1) \cdots 3.2.1$ ولأن p أولي فسيقسم أحد المضاريب

ولكن جميع المضاريب أصغر من p فرضاً إذاً $p \nmid j!$

أي

$$p \mid \binom{p}{j}$$